Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:657.6(476)

Михлюк
Руслан Михайлович

Аудит информационной безопасности на предприятии СООО «СМУ Союзтемфанстрой»

АВТОРЕФЕРАТ
на соискание степени магистра техники и технологии
по специальности 1- 45 81 01 инфокоммуникационные системы и сети

_____

Научный руководитель
Пулко Татьяна Александровна
кандидат технических наук, доцент
кафедры ЗИ

_____

Минск 2017

КРАТКОЕ ВВЕДЕНИЕ

Аудит – форма независимого, нейтрального контроля какого-либо направления деятельности предприятия, широко используемая в практике рыночной экономики. Важным с точки зрения общего развития предприятия является его аудит безопасности, который включает анализ рисков, связанных с возможностью осуществления угроз безопасности, особенно в отношении информационных ресурсов, оценку текущего уровня защищенности информационных систем (ИС), локализацию узких мест в системе их защиты, оценку соответствия ИС существующим стандартам в области информационной безопасности и выработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Выделим основные цели аудита информационной безопасности:

– поиск уязвимостей, позволяющих произвести атаку на информационную систему из внутреннего периметра корпоративной сети;

– определение надежности и достаточности применяемых систем защиты информационной системы от утечек информации;

– регулярное отслеживание изменений в информационной системе;

– предоставление рекомендаций для повышения эффективности механизмов безопасности ИС.

В современных условиях, когда информационные системы пронизывают все сферы деятельности предприятия, а с учетом необходимости их связи с Интернет они оказываются открытыми для реализации внутренних и внешних угроз, проблема информационной безопасности становится не менее важной, чем экономическая или физическая безопасность.

В настоящее время наблюдается повышенный интерес к стандарту ISO/IEC 27001 («Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования») со стороны компаний, работающих в различных отраслях. Соответствие требованиям данного стандарта становится важным фактором коммерческого успеха организации благодаря целому ряду преимуществ, которые она получает.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа по теме магистерской диссертации «Аудит информационной безопасности» выполнялась на предприятии СООО «СМУ Союзтелефонстрой». В настоящее время организация работает с большим объемом информации, как на бумажных, так и электронных носителях, в том числе электронных баз данных и в рамках своей деятельности сталкивается с уникальными рисками в области информационной безопасности.

Основной целью работы было проведение аудита информационной безопасности предприятия изучив самостоятельно основные правовые и законодательные документы действующие в Республике Беларусь, мировые стандарты и методики по данной тематике. По итогу проделанной работы опираясь на полученные теоретические знания в области аудита, был проведен подробный анализ информационной системы предприятия, системы документооборота, системы инженерно-технической защиты с предоставление отчета о проделанной работе в виде основных рекомендаций для руководства предприятия, что повлияло на разработку и внедрение системы менеджмента информационной безопасности (СМИБ), которая позволит обеспечить прочную и надежную основу для инновационного развития предприятия, повышения его конкурентоспособности и обеспечит результативное и экономически эффективное решение следующих задач:

- повышение уровня защищенности важной для предприятия информации;
- оптимизация расходов на информационную безопасность в соответствии с реальными потребностями (в частности, закупаются только необходимые средства защиты);
- приведение в соответствие уровня ИБ как законодательным требованиям, так и требованиям бизнеса;
- повышение доверия инвесторов, заказчиков и партнеров к деятельности предприятия.

Материал диссертации публиковался на XIV Белорусско–российской научно–технической конференции «Технические средства защиты информации» в виде тезиса. И в виде выступления на 52–ой научной конференция аспирантов, магистрантов и студентов Белорусского государственного университета информатики и радиоэлектроники.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Работа содержит следующие пункты: общая характеристика; введение; основы проведения аудита информационной безопасности организации; современные методы и средства аудита информационной безопасности; аудит информационной безопасности предприятия СООО «СМУ Союзтелефонстрой»; заключение; список использованных источников, приложения.

1) Основы проведения аудита информационной безопасности организации. В данном разделе были рассмотрены основные определения аудита и информационной безопасности. Выделены основные цели аудита ИБ, а также задачи, стоящие перед аудитором. Приведена подробная классификация основных видов аудита ИБ с их кратким описание. Перечислены примеры стандартов, на соответствие которым проводится аудит системы ИБ. Определены четыре основных этапа проведения аудита информационной безопасности (разработка регламента, сбор исходных данных, анализ полученных данных с целью оценки текущего уровня безопасности, разработка рекомендаций по повышению уровня защищенности ИС). Приведен перечень исходных данных для аудита и перечислены основные методы сбора исходных данных. Показаны таблицы качественной шкалы оценки уровня ущерба, а также вероятности проведения атаки. Присутствует описание основных рекомендаций для повышения уровня защищенности ИС от угроз (уменьшение риска, уклонение от риска, изменение характера риска, принятие риска).

2) Современные методы и средства аудита информационной безопасности.

Рассмотрены современные методы и средства аудита информационной безопасности (метод CRAMM, программное обеспечение Risk Watch, комплексная система анализа и управления рисками ГРИФ).

3) Аудит информационной безопасности предприятия СООО «СМУ Союзтелефонстрой». В данном разделе приведена краткая характеристика предприятия. Описывается классификация основной информации циркулирующей на предприятии. Рассматриваются основные источники поступления информации. Показана подробная классификация информации по принципу доступности. Опираясь на знания после изучения теоретических знаний в области ИБ разрабатывается план проведения аудита информационной безопасности. Критериями аудита являются стандарт ISO/IEC

27001 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования», ISO/IEC 27002, перечень законодательных и нормативных требований, предъявляемых к СООО «СМУ Союзтелефонстрой».

Кратко описан процесс документооборота на предприятии. В результате чего рекомендуется создание сектора по работе с документами, содержащими конфиденциальную информацию, а также разработку «Инструкции по обеспечению сохранности коммерческих тайн на предприятии».

Проведен анализ организационно-административных мер обеспечения информационной безопасности. Рекомендуется разработать и утвердить положение ИТ-безопасности предприятия с подробным описанием правил для всех видов системной деятельности на предприятии.

Проведен анализ существующей системы компьютерной безопасности. На основании проведенного анализа рекомендовано следующее:

1) В случае необходимости разграничить пользователей в отдельные VLAN, принять меры для резервирования ролей серверов, а также увеличить количество оперативной памяти на рабочих станциях пользователей и серверах.

2) Увеличить быстродействие компьютеров путем обновления «железа» и программного обеспечения.

3) Заменить устаревший малопродуктивный сервисный маршрутизатор d-link DSR-150 на межсетевой экран d-link DFL-210 (способный обрабатывать количество одновременных сессий около 2000) и имеющий небольшую цену.

4) Установить пароли для баз данных специального программного обеспечения.

5) Использовать сторонние программные комплексы шифрование для важных документов, находящихся в свободном доступе на общедоступных ресурсах.

6) Внедрить ИТ регламент по безопасности рабочих мест при отсутствии сотрудника, по проведению вступительных и плановых обучений, по безопасности рабочих станций, по удаленному доступу к рабочим станциям, а также регламент регулирующий права и обязанности пользователей при работе в сети Интернет.

7) Ограничить возможность запуска съемных флэш носителей только тем пользователям, для которых этот доступ необходим.

После проведения анализа существующей системы инженерно-технической защиты информации предложены следующие рекомендации:

1) Внедрить систему СКУД.

2) Закупить и установить контроллеры и электронные замки для каждого

отдельного помещения.

3) Подключить контроллеры дверей к центральной системе СКУД.

4) Настроить систему СКУД согласно техническому заданию, с учетом разрешенных уровней доступа групп сотрудников и времени суток к зонам, где обрабатывается или хранится информация.

5) Зафиксировать группы доступа в регламенте ИТ-безопасности.

6) Регламентировать период проверки прав доступа в зоны безопасности

7) Проводить согласно регламенту проверку прав доступа в зону безопасности.

8) Установить прибор для защиты помещений от прослушивания через акустический и вибрационный каналы в помещении, предназначенном для конфиденциальных переговоров.

9)Использовать технические средства для повышения отказоустойчивости и защиты оборудования от сбоя электропитания.

Проанализировав рекомендации в результате анализа существующей системы инженерно-технической защиты информации и согласовав их пункты с руководством предприятия, было принято для контроля над деятельностью персонала на контрольно-пропускном пункте установить систему контроля и управления доступом (СКУД). Для этого совместно с проектным отделом была создана проектно-сметная документация, выполнен расчет в текущих ценах для определения примерной стоимости работ, и размещение закупки в информационной системе «Тендеры» на сайте информационного республиканского унитарного предприятия «Национальный центр маркетинга и конъюнктуры цен».

Результаты проведенного аудита представлены в виде выводов аудиторского отчета.

ЗАКЛЮЧЕНИЕ

Руководитель предприятия не всегда знает об утечки информации и о последствиях такой утечки. В процессе разработки проекта выяснилось, что основной причиной угроз информационной безопасности на предприятии является человеческий фактор. Данный фактор легко определяется тестом на уровень лояльности сотрудников предприятия с учетом занимаемой должности.

В работе дана общая характеристика предприятия, рассмотрена структура управления предприятия СООО «СМУ Союзтелефонстрой», проведена классификация информации на предприятии, составлена модель злоумышленника. Исследованы информационные потоки, циркулирующие на предприятии.

В исследовательской части работы, проведено тестирование сотрудников предприятия, которое показало, что основным фактором, влияющим на информационную безопасность, является лояльность сотрудников предприятия. Проведен анализ состояния технических средств защиты информации.

Проведенный аудит показало наличие уязвимых мест средств защиты конфиденциальной информации на предприятии. На основании этого были предложены меры совершенствования системы защиты информации.

Разработана комплексная система защиты информации на предприятии СООО «СМУ Союзтелефонстрой».

Сотрудники предприятия стали ответственно относиться к полученным распоряжениям от руководства, улучшилась дисциплина и финансовое положение.

На основании этого следует полагать, что разработка комплекса системы защиты конфиденциальной информации на предприятии не просто вынужденная мера, а прекрасное средство улучшения финансового состояния и является действенным средством в решении повышения уровня безопасности на предприятии в целом.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Михлюк Р.М. Аудит безопасности электронных систем / Р.М. Михлюк // XIV Белорусско–российская научно–техническая конференция «Технические средства защиты информации»: Тезисы докладов – Минск, 2016. – С.11.

2–А. Михлюк Р.М. Аудит информационной безопасности СООО СМУ «Союзтелефонстрой»/ Р.М. Михлюк // 52–ая научная конференция аспирантов, магистрантов и студентов Белорусского государственного университета информатики и радиоэлектроники.